Shared Service Provider Roadmap:
Navigating the Process to Acceptance

Federal Identity Credentialing Committee
Shared Service Provider Subcommittee

Version 1.2
March 5, 2004

Document Control Grid

Document Owner	FICC Shared Service Provider Subcommittee
Contact	Fpki.webmaster@gsa.gov
Document Title	Shared Service Provider Roadmap

Revision History Table

Date	Version	Description	Author
2/18/04	0.9	Final draft version	Dallas N. Bishoff
2/23/04	1.0	Final release version	Dallas N. Bishoff
2/26/04	N/A	Second draft version	NIST PKI Team
3/1/04	1.1	Second release version	SSP Subcommittee
3/5/04	1.2	Third release version	SSP Subcommittee
3/8/04	1.2	Edited	Laura Buell

1.0 Executive Summary

The Shared Service Provider Program is intended to facilitate outsourcing of PKI services by Federal agencies. The Federal government is currently establishing a Qualified Bidders List for vendors that have demonstrated the ability to provide managed PKI services that meet government requirements.[1]

The Shared Service Provider Roadmap is intended to identify the background information, phases, and activities related to the selection process for prospective public key infrastructure (PKI) managed service providers. This document identifies the process by which a vendor qualifies for inclusion on the Qualified Bidders List. The document also describes requirements that must be met to maintain qualification, as well as contracting considerations.

Questions related to this document should be communicated to fpki.webmaster@gsa.gov for consideration.

1.1 Document Overview

This document is constructed in four sections:

- *Shared Service Provider Overview* describes the components of an SSP and the partitioning of responsibility between the SSP and the contracting agency;
- *Shared Service Provider Requirements* describes the steps that vendors must perform before applying for inclusion on the Qualified Bidder List. This section identifies the requirements documents that must be considered as part of this process;
- *Application and Acceptance Process* describes the process by which a vendor applies for inclusion on the Qualified Bidders List and demonstrates that the requirements identified in the preceding section have been satisfied;
- *Post-Acceptance Process* describes the steps a vendor must perform to maintain qualification. In addition, the vendor is required to assist contracting agencies in meeting statutory responsibilities and PKI policy requirements. This section also discusses establishing contract vehicles, such as inclusion on a GSA Schedule 70, to simplify government procurement activities.

1.2 Shared Service Provider Subcommittee

The Shared Service Provider Subcommittee was formed to determine the selection criteria, requirements, processes, and oversight provisions for selection of Shared Service Providers (SSPs) who will act on the government's behalf under the provisions of the

[1] These requirements have been defined by the Shared Services Provider Working Group, which is a subcommittee of the Federal Identity Credentialing Committee (FICC). Statutory authority is derived from the E-Government Act, passing from OMB through the Federal CIO Council (http://www.cio.gov/) to the FICC, and in turn to the FICC Shared Service Provider Subcommittee.

Common Certificate Policy (CCP)[2]. The Subcommittee is composed of various Federal agency representatives. Current Subcommittee membership and publications can be found at http://www.cio.gov/ficc/pki.htm.

2.0 Shared Service Provider Overview

2.1 SSP Components

The SSP program requires four distinct components: Certification Authority (CA); Repository; Archive; and Registration Authority (RA). The responsibilities of the components are described below:

- The Certification Authority (CA) issues X.509 certificates and Certificate Revocation Lists (CRLs).
- The Repository distributes certificates and CRLs.
- The Archive provides long-term secure storage for certificates and CRLs issued by the CA, CA and RA electronic and physical audit logs, audit results, certification and accreditation results, and policy documents.
- The Registration Authority (RA) performs identity proofing for prospective certificate subjects.

2.2 SSP and Contracting Agency

The SSP program is designed to facilitate outsourcing of PKI services by Federal agencies. However, the SSP Subcommittee has designated identity proofing for Federal identity credentials as an agency responsibility. Agencies may contract out RA functions but must maintain responsibility and authority for all decision-making regarding implementation of RA functions and the issuance of credentials.

As a result, outsourcing PKI services creates responsibilities for both the SSP and the contracting agency. These responsibilities include:

- The SSP provides CA, repository, and archive services.
- The SSP develops the Certification Practices Statement covering SSP operations.
- The SSP provides baseline hardware and software to support registration authority operations[3]
- The SSP obtains the compliance audit covering SSP-operated components.
- The SSP performs certification and accreditation to satisfy government C&A requirements.
- The agency is responsible for operating the registration authority component.
- The agency is responsible for identifying which agency employees and affiliates are permitted to obtain credentials.
- The agency obtains the compliance audit covering RA operations.

[2] The CCP is more formally known as the *X.509 Certificate Policy for the Common Policy Framework*, as approved by the Federal PKI Policy Authority.
[3] Agencies are not required to use the SSP-provided baseline RA solution. An agency may wish to leverage an existing infrastructure by integrating current solutions with the SSP offering.

- The agency performs a supplemental accreditation covering agency performed operations.

3.0 Shared Service Provider Requirements

3.1 Policy Requirements

This program is intended to result in the issuance of common physical and electronic credentials (a smart card with PKI certificates) for Federal personnel and other authorized users. To ensure these credentials provide sufficient assurance to satisfy most government-wide application and access control requirements, the Shared Service Provider Requirements reflect two core policy documents approved by the FICC:

- X.509 Certificate Policy for the Common Policy Framework [CCP]
- Federal Smart Card Policy [SCP]

Vendors who operate under the SSP program must operate their PKIs in compliance with the CCP. The CCP specifies three distinct certificate policies: the first covers users with hardware tokens; the second addresses users with software tokens; and the last policy covers devices (e.g., web servers). Vendors who operate under the SSP program must implement the policy covering hardware tokens; the latter two policies are optional.

Vendors are required to have a Certification Practices Statement (CPS) governing the operation of their PKI. The vendor CPS must be in compliance with the CCP and the following supplemental documents:

- X.509 Certificate and CRL Extensions Profile for the Common Policy [PROF]
- Shared Service Provider Repository Service Requirements [REP]
- Archive Requirements for the Managed PKI Service Providers [ARCH]

Vendors are required to obtain a compliance audit[4] from a qualified third party[5] that establishes:

- The vendor CPS is in compliance with the CCP.
- The vendor PKI is operated in compliance with the CPS.

The compliance auditor is required to complete the Common Policy CPS Evaluation Matrix [CPS EVAL] when evaluating vendor CPS compliance with the CCP.

Vendors who operate under the SSP program must implement the mandatory certificate policy with smart cards satisfying the Government Smart Card Interoperability Specification (GSC-IS) Version 2.1 [GSC-IS], as specified in the Federal Smart Card

[4] The vendor is responsible for any expenses associated with compliance audits.
[5] The Federal government requires that the compliance auditor be independent and competent in the field. Vendors may request pre-approval of auditors as a risk management technique.

Policy.[6] Registration authority equipment must support basic smart card requirements (e.g., PIN reset) from the Federal Smart Card Policy.

The FICC is currently developing a third core policy document, the Federal Identity Assurance Policy. If the Federal Identity Assurance Policy establishes more restrictive identity proofing requirements, the CCP will be revised to reflect the new policy. Such changes may necessitate modifications to RA procedures.

3.2 Additional Regulatory Requirements

Federal regulations (e.g., [A-130] and [FISMA]) and supporting documents require that the certification and accreditation process be performed for all government information systems. These regulations apply to both agency-operated systems and managed services. To help agencies meet their regulatory requirements, SSP vendors are required to perform a System Certification[7], as defined in NIST SP 800-37[8] [800-37]. Note that certification and accreditation is performed at the vendor's expense. Vendors are directed to apply the controls commensurate with a FIPS 199 Moderate Impact Level in the accreditation process [FIPS 199]. The System Certification process will create a separate report from the compliance audit described above, but may be performed in parallel. The *FICC Audit Standards for PKI Shared Service Provider Entities* [AUDIT] may help vendors to understand these requirements.

4.0 Application and Acceptance Process

This section outlines the steps required to be accepted for inclusion on the Qualified Bidders List (QBL). The text establishes a preferred ordering of events; the SSP Subcommittee may choose to deviate from this ordering to accelerate the initial population of the QBL.

4.1 Initial Application

The SSP candidate shall submit a written request for evaluation to the point of contact identified in the Notice of Intent. The request shall be accompanied, at a minimum, by the following documents:

- A narrative description of the components for the proposed system, which may include an architectural diagram. This description should fully explain the division of responsibilities between the SSP and the contracting agency.
- A letter from the compliance auditor indicating that the vendor CPS is in compliance with the CCP. The Letter shall be accompanied by the following supporting materials:
    a. The vendor CPS

[6] For more information on GCS-IS, consult NIST Interoperability Report (NISTIR) 6887, which can be found at smartcard.nist.gov.
[7] The certification process will create a reusable C&A report that applies equally to all Federal agencies contracting with that particular SSP.
[8] Note that NIST SP 800-37 is a DRAFT document. Vendors should rely on the current version of 800-37 and any supporting NIST documents when performing certification and accreditation.

b. The completed CPS Analysis Matrix
c. The credentials of the compliance auditor

The Application Package may also include the following documents:

- A letter from the compliance auditor indicating that the vendor PKI is operated in compliance with the CPS.
- An initial System Certification and Accreditation package for review and approval by the Authorizing Official.

Note that these documents are not required to initiate the process but must be reviewed and approved before a vendor can be placed on the Qualified Bidders List. These steps occur in Section 4.3, Review of Completed Application. Vendors are encouraged to submit complete application packages to expedite the process.

A checklist, "Application for Inclusion on the Qualified Bidders List for PKI Service Providers", will be available at http://www.cio.gov/ficc/pki.htm to assist in completing the application process.

4.2 Operational Capability Demonstration

Upon receipt of an acceptable application package, the FICC will contact the SSP candidate to arrange for an Operational Capability Demonstration (OCD).

The OCD is the process by which the government validates the ability of an SSP candidate to operate a PKI environment that is compliant with the Common Certificate Policy (CCP) and the supplemental documents specified in Section 3.1. The "Operational Capabilities Demonstration Criteria for Shared Service Provider Candidates" specifies the functionality to be demonstrated during the OCD.

The vendor OCD shall be approved if the government determines that all OCD criteria were successfully demonstrated.

If the government determines that criteria in the OCD were not successfully demonstrated, the vendor will be provided with a list of criteria that were not met. Depending upon the severity of the issues, the government may choose from the following options:

- If the issues are judged to be minor, the SSP subcommittee may accept a written attestation that the issues have been corrected and approve the OCD.
- The SSP Subcommittee may require that the vendor perform a new OCD.

If remediation requires a change to the CPS, the government will also require an update to the compliance audit.

4.3 Government Review of Completed Application

After receipt of a completed application package, including the audit letter covering SSP operations and the Certification package, the FICC will initiate government review of the compliance analysis and Certification documentation.

Note that these steps may be performed in parallel with the OCD if the audit letter covering SSP operations and the Certification package are included in the initial application.

4.3.1 Compliance Analysis

The SSP Subcommittee will review the compliance letter with the supporting materials. The SSP Subcommittee may recommend approval of the compliance audit, recommend rejection of the compliance audit, or ask for further clarifications. The FICC Chair will consider the SSP Subcommittee's recommendation and vote to approve or reject the compliance audit.

4.3.2 Certification

The authorizing official will review the submitted System Certification and Accreditation package.[9] The package covers both the SSP operated components and the SSP-supplied RA hardware and software. The authorizing official may fully authorize the system to process government data, grant interim approval to process government data, or deny authorization to operate.

4.4 Qualified Bidders List

Upon approval of the vendor OCD (see Section 4.2), the compliance analysis (see Section 4.3.1), and authorization of the SSP (see Section 4.3.2), the FICC Chair shall add the vendor to the Qualified Bidders List.

5.0 Post-Acceptance Process

5.1 Contract Execution Activities

Companies on the Qualified Bidders List will be invited to submit proposals for newly established Special Item Numbers (SINs) on the Group 70 Schedule. Entities placed on the Qualified Bidders List who already provide PKI services under a GSA Schedule Contract or other Government-Wide Acquisition Contract (GWAC) will not be required to obtain another contract to deliver services. Depending upon the scope of the existing contract, contract modifications may be necessary to provide a complete solution under the Common Certificate Policy. If the necessary contract modifications exceed the scope of the already awarded contract, the companies will be invited to submit a Group 70 Schedule proposal.

[9] The government has not yet identified the authorizing official for the certification and accreditation.

Qualified Bidders are encouraged to include additional services in contract vehicles. Examples include:

- Custom integration activities to support integrating the SSP with agency-owned equipment and PKI-enabling agency applications.
- RA and end-user training.
- Policy development services for agencies that maintain an agency-specific Registration Practices Statement (RPS). See [RA REQ] for details regarding the contents of an RPS.

5.2 Recurring Activities

5.2.1 Yearly Compliance Audit

The CCP mandates yearly compliance audits performed by a competent, independent third party.

The SSP shall submit a compliance audit yearly covering SSP-operated components. Compliance audits shall be processed as in Section 4.3.1. If an SSP is determined to be out of compliance, they shall submit a remediation plan to the SSP Subcommittee.[10]

5.2.2 Certification and Accreditation Maintenance Process

OMB A-130 requires that the certification and accreditation process be repeated every three years, or whenever there is a major modification to the system.

5.3 SSP - Agency Interaction

5.3.1 Agency Audit

Each agency that obtains services from an SSP must obtain and submit a compliance audit covering registration authorities and any other agency operated components. The SSP must provide the Agency with sufficient information regarding SSP-provided equipment to facilitate this process.

5.3.2 Agency System Accreditation

Agency certification and accreditation requirements are not fully satisfied by the SSP certification and accreditation. The agency must perform an agency-specific certification and accreditation based on the SSP authorization and agency operation of RA components.

5.3.3 Policy Coordination

The Federal Contracting Agency and the SSP vendor are jointly responsible for meeting the requirements in the CCP. To ensure these policy requirements are met, vendors and agencies must ensure that CA and RA procedures are consistent and complete.

[10] Each agency that obtains services from an SSP must obtain and submit a compliance audit covering registration authorities and any other agency-operated components.

In particular, the agency must operate the registration authority component as documented in either the SSPs CPS, or develop a Registration Practices Statement (RPS) that covers these functions.

5.3.4 Agency Archive Requirements

The agency is responsible for (1) developing a records management plan that will meet its regulatory, legal, and business needs as well as the SSP archive requirements [ARCH], (2) obtaining NARA approval of its plan, (3) conveying that plan's archival requirements to the SSP, and (4) assuring that the SSP is capable of fulfilling those agency requirements and understands its obligation as an SSP to do so.

6.0 References

[800-37] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* Draft Version 2 June 2003. Available at <http://csrc.nist.gov/publications/drafts/sp800-37-Draftver2.pdf>

[A-130] Office of Management and Budget Circular A-130, Revised (Transmittal 4). Available at <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

[AUDIT] *FICC Audit Standards for PKI Shared Service Provider Entities*, 16 January 2004. Available at <http://www.cio.gov/ficc/documents/AuditStandards.pdf>

[ARCH] *Archive Requirements For Managed PKI Service Providers*, 7 February 2004. Available at <http://www.cio.gov/ficc/documents/ArchiveRqmtsForSSP.pdf>

[CCP] *X.509 Certificate Policy for the Common Policy Framework*, 10 February 2004. Available at <http://www.cio.gov/ficc/documents/CommonPolicy.pdf>

[CPS EVAL] *CPS Evaluation Matrix For Evaluation Against the Requirements for the Common Policy Framework Version 1.1*, 21 December 2003. Available at <http://www.cio.gov/ficc/documents/CPSmatrix.pdf>

[FISMA] *Federal Information Security Management Act of 2002 (Title III of E-Gov),* Available at <http://csrc.nist.gov/policies/FISMA-final.pdf>

[GSC-IS] NISTIR 6887 *Government Smart Card Interoperability Specification (GCS-IS) Version 2.1*. Available at <http://csrc.nist.gov/publications/nistir/nistir-6887.pdf>

[OCD] *Operational Capabilities Demonstration Criteria for Shared Services Provider Candidates*. Available at <http://www.cio.gov/ficc/documents/OCDcriteria.pdf>

[PROF] *X.509 Certificate and CRL Extensions Profile for the Common Policy*, December 22, 2003. Available at <http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf>

[RA REQ] Registration Authority (RA) Requirements. Available at <http://www.cio.gov/ficc/documents/RArequirements.pdf>

[REP] *Shared Service Provider Repository Service Requirements*, January 23, 2004. Available at <http://www.cio.gov/ficc/documents/SSPrepositoryRqmts.pdf>

[SCP] *Policy Issuance Regarding Smart Cards Systems For Identification and Credentialing of Employees*, February 2004. Available at <http://www.smart.gov/smartgov/information/scpfinal2004.doc>